

IN THE CLAIMS

This listing of claims replaces all prior listings:

1. (Currently Amended) A content distribution system for performing content transaction management utilizing an encrypted data packet in the form of a secure container, comprising:

 a content provider which generates the secure container including a first section and a second section[;], and

 a plurality of user devices configured to receive the secure container from the content provider[;], and

 the secure container,

 wherein,

 the secure container contains a content encrypted by a content key and container information including conditions relating to a transaction of the content,

 the first section of the secure container contains information relating to transmitting said secure container to the plurality of user devices,

 the second section of the secure container includes a person identification certificate (IDC) and an IDC identifier list to authenticate a user when said secure container is transmitted to said plurality of user devices,

 the IDC includes a biometric information template encrypted in one of a plurality of manners which is identifiable in the IDC identifier list,

 one of the user devices is a secure container distributing device which (1) receives a primary distribution including the secure container from the content provider and verifies the authenticity of the secure container, (2) decrypts and extracts the encrypted biometric information template stored in the IDC, and (3) is configured to compare sampling information input by a user of a receiving device which is one of the user devices with the decrypted biometric information template to authenticate the user of the receiving device,

the secure container distributing device initiates a secondary distribution after the primary distribution by sending the content key to the receiving device, and

the receiving device decrypts and copies the content sent from said secure container distributing device, after the user of the receiving device is authenticated.

2. (Previously Presented) The content distribution system according to Claim 1, wherein

the receiving device generates usage control status information relating to the content included in said secure container, and

the receiving device stores the usage control status information including the IDC identifier list in a memory of the receiving device.

3. (Previously Presented) The content distribution system according to Claim 1, wherein

the receiving device generates usage control status information relating to the content based included in said secure container, and stores the usage control status information, which includes the IDC identifier list, in a memory of the receiving device, and

the usage control status information includes conditions relating to processing the secondary distribution of the content after the primary content distribution.

4. (Previously Presented) The content distribution system according to Claim 1, wherein

the secure container distributing device is configured to authenticate the user of the receiving device by comparing sampling information input by a user of the receiving device with the biometric information template, and

the secure container distributing device makes the content is available to the receiving device, after the user of the receiving device is authenticated.

5. (Cancelled).

6. (Previously Presented) The content distribution system according to Claim 1, wherein a

the secure container distributing device is configured to authenticate a the user of the receiving device by comparing sampling information input by a user of the receiving device with the biometric information template,

the secure container distributing device notifies the content provider of the authentication result, and

the secure container distributing device is configured to make the content available to the receiving device, after the user of the receiving device is authenticated.

7. (Previously Presented) The content distribution system according to Claim 1, wherein

the secure container distributing device is configured to authenticate a user of the receiving device by comparing sampling information input by a user of the receiving device with the template stored in the IDC, and

the secure container distribution device notifies the content provider of the authentication result, and

the distributing device is configured to distribute said secure container and said content key stored in said secure container to the receiving device and to make the secure container available at the receiving device, after the user of the receiving device is authenticated.

8. (Previously Presented) The content distribution system according to Claim 1, wherein the IDC is stored in advance on any of said plurality of user devices which performs authentication.

9. (Previously Presented) The content distribution system according to Claim 1, wherein any of said user devices authenticates the user of the user device transmitting the secure container, and

any of said plurality of user devices is configured to obtain the IDC.

10. (Previously Presented) The content distribution system according to Claim 1, wherein the container information includes content usage permission data, and

the receiving device is configured to restrict usage of the content based on the content usage permission data or usage control status information.

11. (Previously Presented) The content distribution system according to Claim 1, wherein said secure container includes a digital signature of the device sending said secure container.

12. (Previously Presented) The content distribution system according to Claim 1, wherein the IDC identifier list includes data effective to associate a user identifier with his/her IDC identifier.

13. (Previously Presented) The content distribution system according to Claim 1, wherein the content provider, the secure container distributing device and the receiving devices include an encryption unit effective to mutually authenticate a data transmission between any two of the content provider, the secure container distributing device or the receiving devices, and

the data transmitting and receiving sides are configured, respectively, to generate a digital signature of the transmitting data and to verify the digital signature.

14. (Previously Presented) The content distribution system according to Claim 1, wherein the biometric information template comprises at least any one of the following

Response to April 9, 2008 Office Action

Application No. 09/943,773

Page 6

fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information.

15. – 31. (Cancelled).